CheckPoint

156-115.77 Exam

Check Point Certified Security Master

Question: 1

What command would you use for a packet capture on an absolute position for TCP streaming (out) 1ffffe0

A. fw ctl chain -po 1ffffe0 -o monitor.out
B. fw monitor -po -0x1ffffe0 -o monitor.out
C. fw monitor -e 0x1ffffe0 -o monitor.out
D. fw monitor -pr 1ffffe0 -o monitor.out

Answer: B

Question: 2

The command fw monitor -p all displays what type of information?

A. It captures all points of the chain as the packet goes through the firewall kernel.
B. This is not a valid command.
C. The -p is used to resolve MAC address in the firewall capture.
D. It does a firewall monitor capture on all interfaces.

Answer: A

Question: 3

What does the IP Options Strip represent under the fw chain output?

A. IP Options Strip is not a valid fw chain output.
B. The IP Options Strip removes the IP header of the packet prior to be passed to the other kernel functions.
C. The IP Options Strip copies the header details to forward the details for further IPS inspections.
D. IP Options Strip is only used when VPN is involved.

Answer: B

Question: 4

The command that lists the firewall kernel modules on a Security Gateway is:

A. fw list kernel modules
B. fw ctl kernel chain
C. fw ctl debug -m
D. fw list modules

Answer: C

Question: 5

Which of the following BEST describes the command fw ctl chain function?

A. View how CoreXL is distributing traffic among the firewall kernel instances.
B. View established connections in the connections table.
C. View the inbound and outbound kernel modules and the order in which they are applied.
D. Determine if VPN Security Associations are being established.

Answer: C

Question: 6

The command _____ shows which firewall chain modules are active on a gateway.

A. fw stat
B. fw ctl debug
C. fw ctl chain
D. fw ctl multik stat

Answer: C

Question: 7

The command fw ctl kdebug <params> is used to:

A. list enabled debug parameters.
B. read the kernel debug buffer to obtain debug messages.
C. enable kernel debugging.
D. select specific kernel modules for debugging.

Answer: B

Question: 8

Compare these two images to establish which blade/feature was disabled on the firewall.

A. IPS
B. VPN
C. NAT
D. L2TP

Answer: B

Question: 9

What command would give you a summary of all the tables available to the firewall kernel?

A. fw tab
B. fw tab -s
C. fw tab -h
D. fw tab -o

Answer: B

Question: 10

What flag option(s) must be used to dump the complete table in friendly format, assuming there are more than one hundred connections in the table?

A. fw tab -t connections -f
B. fw tab -t connect -f -u
C. fw tab -t connections -s

D. fw tab -t connections -f –u

Answer: B

Question: 11

Which directory below contains the URL Filtering engine update info? Here you can also go to see the status of the URL Filtering and Application Control updates.

A. $FWDIR/urlf/update
B. $FWDIR/appi/update
C. $FWDIR/appi/urlf
D. $FWDIR/update/appi

Answer: B

Question: 12

For URL Filtering in the Cloud in R75 and above, what table is used to contain the URL Filtering cache values?

A. urlf_blade_on_gw
B. urlf_cache_tbl
C. urlf_cache_table
D. url_scheme_tab

Answer: C

Question: 13

You are troubleshooting a Security Gateway, attempting to determine which chain is causing a problem. What command would you use to show all the chains through which traffic passed?

A. [Expert@HostName]# fw ctl chain
B. [Expert@HostName]# fw monitor -e "accept;" -p all
C. [Expert@HostName]# fw ctl debug –m
D. [Expert@HostName]# fw ctl zdebug all

Answer: B

Question: 14

True or False: Software blades perform their inspection primarily through the kernel chain modules.

A. False. Software blades do not pass through the chain modules.
B. True. Many software blades have their own dedicated kernel chain module for inspection.

C. True. All software blades are inspected by the IP Options chain module.
D. True. Most software blades are inspected by the TCP streaming or Passive Streaming chain module.

Answer: B

Question: 15

When using the command fw monitor, what command ensures the capture is accurate?

A. export TDERROR_ALL_ALL=5
B. fwaccel off
C. fwaccel on
D. fw accel off

Answer: B

Thank You for trying 156-115.77 PDF Demo

To Buy Latest 156-115.77 Exam Full Version visit link below

https://www.certkillers.net/Exam/156-115.77

Start Your 156-115.77 Preparation

[Limited Time Offer] Use Coupon "CKNET" for further discount on your purchase. Test your 156-115.77 preparation with actual exam questions.